

PIN Self-Assessment Questionnaire (SAQ)

For PCI PIN Security Requirements Version 2

Last Updated: March 2015

Contents

[Overview 4](#_Toc415651441)

[PCI PIN Environment & Contact Information 5](#_Toc415651442)

[PCI PIN Security Compliance Statement 9](#_Toc415651443)

[PCI PIN Security Assessment Technical Requirements 10](#_Toc415651444)

[CONTROL OBJECTIVE 1 10](#_Toc415651445)

[CONTROL OBJECTIVE 2 13](#_Toc415651446)

[CONTROL OBJECTIVE 3 15](#_Toc415651447)

[CONTROL OBJECTIVE 4 17](#_Toc415651448)

[CONTROL OBJECTIVE 5 21](#_Toc415651449)

[CONTROL OBJECTIVE 6 23](#_Toc415651450)

[CONTROL OBJECTIVE 7 28](#_Toc415651451)

[Normative Annex A – Symmetric Key Distribution using Asymmetric Techniques 32](#_Toc415651452)

[A1 – Remote Key Distribution Using Asymmetric Techniques Operations 32](#_Toc415651453)

[CONTROL OBJECTIVE 1 32](#_Toc415651454)

[CONTROL OBJECTIVE 2 32](#_Toc415651455)

[CONTROL OBJECTIVE 3 32](#_Toc415651456)

[CONTROL OBJECTIVE 4 32](#_Toc415651457)

[CONTROL OBJECTIVE 5 33](#_Toc415651458)

[CONTROL OBJECTIVE 6 33](#_Toc415651459)

[Normative Annex A – Symmetric Key Distribution using Asymmetric Techniques 35](#_Toc415651460)

[A2 – Certification and Registration Authority Operations 35](#_Toc415651461)

[CONTROL OBJECTIVE 3 35](#_Toc415651462)

[CONTROL OBJECTIVE 4 35](#_Toc415651463)

[CONTROL OBJECTIVE 5 36](#_Toc415651464)

[CONTROL OBJECTIVE 7 42](#_Toc415651465)

[Normative Annex B – Key-Injection Facilities 47](#_Toc415651466)

[Key-Injection Facility Security Requirements Technical Reference 47](#_Toc415651467)

[CONTROL OBJECTIVE 1 47](#_Toc415651468)

[CONTROL OBJECTIVE 2 48](#_Toc415651469)

[CONTROL OBJECTIVE 3 50](#_Toc415651470)

[CONTROL OBJECTIVE 4 52](#_Toc415651471)

[CONTROL OBJECTIVE 5 58](#_Toc415651472)

[CONTROL OBJECTIVE 6 59](#_Toc415651473)

[CONTROL OBJECTIVE 7 66](#_Toc415651474)

[PCI PIN Security Requirements Exception Form 70](#_Toc415651475)

# Overview

This document contains the necessary information for an organization performing a self-assessment to record compliance with the Payment Card Industry (PCI) PIN Security Requirements Version 2.0 Technical Requirements, requirements for Symmetric Key Distribution using Asymmetric Techniques and/or requirements for Key Injection Facilities (KIFs). It must be used in conjunction with PCI PIN Security Requirements and Testing Procedures Version 2.0, dated December 2014.

Contents include:

1. PCI PIN Security Compliance

* General organization information
* Processing environment
* Compliance statement for organization

1. PCI PIN Security Assessment Questions
2. PCI PIN Security Requirements Exception Form

# PCI PIN Environment & Contact Information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Part 1. Organization Information** | | | | | |
| **Organization Information** | | | | | |
| Company Name: |  | Title: |  | | |
| Contact Name: |  | E-mail: |  | | |
| Telephone: |  | Fax: |  | | |
| Business Address: |  | City: |  | | |
| State/Province: |  | | | |
| Country: |  | Zip: |  |
| Visa Business ID : 10       If applicable | | | | | |
| Name of Sponsoring Institution(s) and Contacts *if applicable*: | | | | | |
| 1. Name: | | | | | |
| Contact: | | | | | |
| 1. Name: | | | | | |
| Contact: | | | | | |
| 1. Name: | | | | | |
| Contact: | | | | | |

|  |  |
| --- | --- |
| Date of Review: |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **PIN Reviewer Information** | | | | | | | |
| Name: |  | | | | | | |
| Title: |  | | | | | | |
| Telephone: |  | | | E-mail: |  | | |
| Business Address: |  | | | City: |  | | |
| State/Province: |  | Country: |  | | | Zip: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Part 2. Processing Environment** | | | |
| 1. **Organization Description *(check one)*** | | | |
| Certificate Authority: |  | Acquirer: |  |
| Encryption Service Organization (ESO) |  | Third Party Processor |  |
| Other: |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Do you process PIN-based transactions (drive ATMs or POS devices, or act in as a switch to interchange networks?** | | | |
| Yes: |  | No: |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Does a third-party processor process your interchange PIN-based transactions?** | | | | |
| Yes: |  | | No: |  |
| If Yes, by whom? | |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Does your organization perform any of the following Key Management functions?** | | | |
| 1. Loading keys/initializing ATM’s and/or Point of Sale (POS) devices? | | | |
| Yes: |  | No: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Creating keys and/or key components for ATM’s, POS or host security modules? | | | |
| Yes: |  | No: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Conveying keys or key components to ATM/POS initialization personnel or to networks with whom you connect? | | | |
| Yes: |  | No: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Storing keys or key components? | | | |
| Yes: |  | No: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Destroying keys or key components? | | | |
| Yes: |  | No: |  |

|  |
| --- |
| **Part 2. Processing Environment - continued** |
| 1. **Do you have *written* documentation for the functions in the previous question for which you answered yes? Please check those for which you have documentation.** |
| 1. b.  c.  d.  e. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Include Payment Transaction Security (PTS) Approved Devices** | | | | | | |
| ATM | POS | Manufacture | Model No. | Hardware # | Firmware # | Approx. Quantity |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |
| --- |
| 1. **If you process your own PIN-based transactions or PIN-based transactions for others (answered “Yes” to question 2), please answer the following:** |
| 1. CPU/Operating System (release level) platforms used for PIN processing: |

|  |
| --- |
| 1. Security Software: |

|  |
| --- |
| 1. Application software: |
| To drive devices: |
| For switches : |

|  |  |  |
| --- | --- | --- |
| 1. Hardware (host) Security Module(s) used to security encryption keys and perform PIN translation: | | |
| Manufacture | Model No. | Approximate Quantity |
|  |  | Production:       Test: |
|  |  | Production:       Test: |
|  |  | Production:       Test: |

|  |
| --- |
| **Part 2. Processing Environment - continued** |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Do you have access to the source code for the application software? | | | |
| Yes: |  | No: |  |

|  |
| --- |
| 1. Estimated annual number of online PIN-based Interchange transactions for Visa Branded Products (Visa/Plus/Interlink/Visa Electron): |
| ATM: |
| POS: |

|  |
| --- |
| 1. Estimated annual number of key injections/ key loading: |
| ATM: |
| POS: |
| 1. **List all Interchange networks and / or processors with which you connect:** |
|  |

|  |
| --- |
| PCI PIN Security Compliance Statement |

**PIN Reviewer**

I,

*(Print or type name and title)*

*(Check one)*

am an **internal auditor** for       and I have no operational responsibility for matters referenced in the PCI PIN Security Requirements Self-Assessment.

am an **independent auditor** employed by       and hired by       to complete the PCI PIN Security Requirements Self-Assessment.

am a **security or compliance professional** for       and I have no operational responsibility for matters referenced in the PCI PIN Security Requirements Self-Assessment.

I do hereby attest that the above-referenced organization is:

*(Check one)*

**In full compliance** with the PCI PIN Security Requirements Self-Assessment.

**Not in full compliance** as indicated by the attached Exception Form(s).

Signature:      Date:

# PCI PIN Security Assessment Technical Requirements

This document must be used in conjunction with the [PCI PIN Security Requirements and Test Procedures Version 2.0](https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_v2_audit_techniques_Dec_2014_c.pdf). The reviewer must pay special attention and follow the testing procedures specified to ensure consistent review and adherence to requirements.

Each requirements must have a response of “Yes”, “No” or “N/A”. “No” and “N/A” answers must be explained in writing. The testing procedures defined in the PCI PIN Security Requirements and Test Procedures Version 2.0 may include multiple steps that must be performed to confirm compliance. All steps must be performed in order to determine compliance to the requirement. Non-compliance to any of the requirements must be documented on the PCI PIN Security Requirements Exception Form, included in this document. The exception form may be reproduced when multiple items as required.

## CONTROL OBJECTIVE 1

***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 1: All cardholder-entered PINs must be processed in equipment that conforms to the requirements for secure cryptographic devices (SCDs). PINs must never appear in the clear outside of an SCD.*** | | |
| A secure cryptographic device (SCD) must meet the requirements of a “Physically Secure Device” as defined in ISO 9564. For POI PIN-acceptance devices this is evidenced by their being validated and PCI approved against one of the following:   * One of the versions of the PCI PTS standard, as members of Approval Classes EPP, PED, or UPT (collectively known as POI Devices) and Approval Class HSMs, or * FIPS 140-2 level 3 or higher | | |
| **1-1** | **Yes No N/A** | **Remarks:** |
| * 1. *Not used in core requirements and testing procedures* |  | |
| **1-3** | **Yes No N/A** | **Remarks:** |
| **1-4** | **Yes No N/A** | **Remarks:** |
| ***Requirement: 2a. Cardholder PINs shall be processed in accordance with approved standards.***  ***a. All cardholder PINs processed online must be encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double-length keys.***  ***b. All cardholder PINs processed offline using IC card technology must be protected in accordance with the requirements in Book 2 of the* EMV IC Card Specifications for Payment Systems *and ISO 9654.*** | | |
| **2-1** | **Yes No N/A** | **Remarks:** |
| **2-2** | **Yes No N/A** | **Remarks:** |
| **2-3** | **Yes No N/A** | **Remarks:** |
| **2-4** | **Yes No N/A** | **Remarks:** |
| ***Requirement 3: For online interchange transactions, PINs must be only encrypted using ISO 9564–1 PIN-block formats 0, 1, 3 or 4. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.*** | | |
| **3-1** | **Yes No N/A** | **Remarks:** |
| **3-2** | **Yes No N/A** | **Remarks:** |
| **3-3** | **Yes No N/A** | **Remarks:** |
| ***Requirement 4: PINs must not be stored except as part of a store-and-forward transaction, and only for the minimum time necessary. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged.*** | | |
| **4-1** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 2

***Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 5: All keys and key components must be generated using an approved random or pseudo-random process.*** | | |
| **5-1** | **Yes No N/A** | **Remarks:** |
| ***Requirement 6: Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.*** | | |
| **6-1** |  | |
| **6-1.1** | **Yes No N/A** | **Remarks:** |
| **6-1.2** | **Yes No N/A** | **Remarks:** |
| **6-1.3** | **Yes No N/A** | **Remarks:** |
| **6-1.4** | **Yes No N/A** | **Remarks:** |
| **6-1.5** | **Yes No N/A** | **Remarks:** |
| **6-2** | **Yes No N/A** | **Remarks:** |
| **6-3** | **Yes No N/A** | **Remarks:** |
| **6-4** | **Yes No N/A** | **Remarks:** |
| **6-5** | **Yes No N/A** | **Remarks:** |
| **6-6** | **Yes No N/A** | **Remarks:** |
| ***Requirement 7: Documented procedures must exist and be demonstrably in use for all key-generation processing.*** | | |
| **7-1** | **Yes No N/A** | **Remarks:** |
| **7-2** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 3

***Keys are conveyed or transmitted in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 8: Secret or private keys shall be transferred by:***   1. ***Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or*** 2. ***Transmitting the key in ciphertext form.***   ***Public keys must be conveyed in a manner that protects their integrity and authenticity.*** | | |
| **8-1** | **Yes No N/A** | **Remarks:** |
| **8-2** | **Yes No N/A** | **Remarks:** |
| **8-3** | **Yes No N/A** | **Remarks:** |
| **8-4** | **Yes No N/A** | **Remarks:** |
| ***Requirement 9: During its transmission, conveyance, or movement between any two organizational entities, any single unencrypted secret or private key component must at all times be protected.***  ***Sending and receiving entities are equally responsible for the physical protection of the materials involved.*** | | |
| **9-1** | **Yes No N/A** | **Remarks:** |
| **9-2** | **Yes No N/A** | **Remarks:** |
| **9-3** | **Yes No N/A** | **Remarks:** |
| **9-4** | **Yes No N/A** | **Remarks:** |
| **9-5** | **Yes No N/A** | **Remarks:** |
| ***Requirement 10: All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.*** | | |
| **10-1** | **Yes No N/A** | **Remarks:** |
| ***Requirement 11: Documented procedures must exist and be demonstrably in use for all key transmission and conveyance processing.*** | | |
| **11-1** | **Yes No N/A** | **Remarks:** |
| **11-2** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 4

***Key loading to HSMs and PIN entry devices is handled in a secure manner12***

|  |  |  |
| --- | --- | --- |
| ***Requirement 12: Secret and private keys must be input into hardware (host) security modules (HSMs) and PIN entry devices (PEDs) in a secure manner.***   * + 1. ***Unencrypted secret or private keys must be entered using the principles of dual control and split knowledge.***     2. ***Key-establishment techniques using public-key cryptography must be implemented securely*** | | |
| **12-1** | **Yes No N/A** | **Remarks:** |
| **12-2** | **Yes No N/A** | **Remarks:** |
| **12-3** | **Yes No N/A** | **Remarks:** |
| **12-4** | **Yes No N/A** | **Remarks:** |
| **12-5** | **Yes No N/A** | **Remarks:** |
| **12-6** | **Yes No N/A** | **Remarks:** |
| **12-7** | **Yes No N/A** | **Remarks:** |
| **12-8** | **Yes No N/A** | **Remarks:** |
| ***Requirement 13: The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.*** | | |
| **13-1** | **Yes No N/A** | **Remarks:** |
| **13-2** | **Yes No N/A** | **Remarks:** |
| **13-3** | **Yes No N/A** | **Remarks:** |
| **13-4** | **Yes No N/A** | **Remarks:** |
| **13-4.1** | **Yes No N/A** | **Remarks:** |
| **13-4.2** | **Yes No N/A** | **Remarks:** |
| **13-4.3** | **Yes No N/A** | **Remarks:** |
| **13-4.4** | **Yes No N/A** | **Remarks:** |
| **13-5** | **Yes No N/A** | **Remarks:** |
| **13-6** | **Yes No N/A** | **Remarks:** |
| **13-7** | **Yes No N/A** | **Remarks:** |
| **13-8** | **Yes No N/A** | **Remarks:** |
| ***Requirement 14: All hardware and access/authentication mechanisms (e.g., passwords) used for key loading must be managed under the principle of dual control.*** | | |
| **14-1** | **Yes No N/A** | **Remarks:** |
| **14-2** | **Yes No N/A** | **Remarks:** |
| **14-3** | **Yes No N/A** | **Remarks:** |
| **14-4** | **Yes No N/A** | **Remarks:** |
| **14-5** | **Yes No N/A** | **Remarks:** |
| ***Requirement 15: The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*** | | |
| **15-1** | **Yes No N/A** | **Remarks:** |
| **15-2** | **Yes No N/A** | **Remarks:** |
| ***Requirement 16: Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.*** | | |
| **16-1** | **Yes No N/A** | **Remarks:** |
| **16-2** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 5

***Keys are used in a manner that prevents or detects their unauthorized usage.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 17: Unique, secret cryptographic keys must be in use for each identifiable link between host computer systems between two organizations or logically separate systems within the same organization.*** | | |
| **17-1** | **Yes No N/A** | **Remarks:** |
| ***Requirement 18: Unique, secret cryptographic keys must be in use for each identifiable link between host computer systems between two organizations or logically separate systems within the same organization.*** | | |
| **18-1** | **Yes No N/A** | **Remarks:** |
| **18-2** | **Yes No N/A** | **Remarks:** |
| **18-3** | **Yes No N/A** | **Remarks:** |
| ***Requirement 19: Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*** | | |
| **19-1** | **Yes No N/A** | **Remarks:** |
| **19-2** | **Yes No N/A** | **Remarks:** |
| **19-3** | **Yes No N/A** | **Remarks:** |
| **19-4** | **Yes No N/A** | **Remarks:** |
| **19-5** | **Yes No N/A** | **Remarks:** |
| ***Requirement 20: All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (e.g., PED) that processes PINs must be unique (except by chance) to that device*** | | |
| **20-1** | **Yes No N/A** | **Remarks:** |
| **20-2** | **Yes No N/A** | **Remarks:** |
| **20-3** | **Yes No N/A** | **Remarks:** |
| **20-4** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 6

***Keys are administered in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 21: Secret keys used for enciphering PIN-encryption keys or for PIN encryption, or private keys used in connection with remote key- distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*** | | |
| **21-1** | **Yes No N/A** | **Remarks:** |
| **21-2** | **Yes No N/A** | **Remarks:** |
| **21-2.1** | **Yes No N/A** | **Remarks:** |
| **21-2.2** | **Yes No N/A** | **Remarks:** |
| **21-2.3** | **Yes No N/A** | **Remarks:** |
| **21-2.4** | **Yes No N/A** | **Remarks:** |
| **21-3** | **Yes No N/A** | **Remarks:** |
| **21-3.1** | **Yes No N/A** | **Remarks:** |
| **21-3.2** | **Yes No N/A** | **Remarks:** |
| **21-3.3** | **Yes No N/A** | **Remarks:** |
| ***Requirement 22: Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key, its subsidiary keys (those keys encrypted with the compromised key), and keys derived from the compromised key, to a value not feasibly related to the original key.*** | | |
| **22-1** | **Yes No N/A** | **Remarks:** |
| **22-1.1** | **Yes No N/A** | **Remarks:** |
| **22-1.2** | **Yes No N/A** | **Remarks:** |
| **22-1.3** | **Yes No N/A** | **Remarks:** |
| **22-1.4** | **Yes No N/A** | **Remarks:** |
| **22-1.5** | **Yes No N/A** | **Remarks:** |
| **22-2** | **Yes No N/A** | **Remarks:** |
| ***Requirement 23: Keys generated using reversible key-calculation methods, such as key variants, must only be used in SCDs that possess the original key.***  ***Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange must not be used as a working key or as a Master File Key for local storage.***  ***Keys generated using a non-reversible process, such as key-derivation or transformation process with a base key using an encipherment process, are not subject to these requirements.*** | | |
| **23-1** | **Yes No N/A** | **Remarks:** |
| **23-2** | **Yes No N/A** | **Remarks:** |
| **23-3** | **Yes No N/A** | **Remarks:** |
| ***Requirement 24: Secret and private keys and key components that are no longer used or have been replaced must be securely destroyed.*** | | |
| **24-1** | **Yes No N/A** | **Remarks:** |
| **24-2** | **Yes No N/A** | **Remarks:** |
| **24-2.1** | **Yes No N/A** | **Remarks:** |
| **24-2.2** | **Yes No N/A** | **Remarks:** |
| **24-2.3** | **Yes No N/A** | **Remarks:** |
| ***Requirement 25: Access to secret and private cryptographic keys and key material must be:***   * + 1. ***Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and***     2. ***Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.*** | | |
| **25-1** | **Yes No N/A** | **Remarks:** |
| **25-1.1** | **Yes No N/A** | **Remarks:** |
| **25-1.2** | **Yes No N/A** | **Remarks:** |
| **25-1.3** | **Yes No N/A** | **Remarks:** |
| **25-1.4** | **Yes No N/A** | **Remarks:** |
| ***Requirement 26: Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD.*** | | |
| **26-1** | **Yes No N/A** | **Remarks:** |
| ***Requirement 27: Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.***  ***Note: It is not a requirement to have backup copies of key components or keys.*** | | |
| **27-1** | **Yes No N/A** | **Remarks:** |
| **27-2** | **Yes No N/A** | **Remarks:** |
| ***Requirement 28: Documented procedures must exist and must be demonstrably in use for all key-administration operations.*** | | |
| **28-1** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 7

***Equipment used to process PINs and keys is managed in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 29: PIN-processing equipment (e.g., POI devices and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the deployment of the device—both prior to and subsequent to the loading of cryptographic keys—and that precautions are taken to minimize the threat of compromise once deployed.*** | | |
| **29-1** | **Yes No N/A** | **Remarks:** |
| **29-1.1** | **Yes No N/A** | **Remarks:** |
| **29-1.1.1** | **Yes No N/A** | **Remarks:** |
| **29-1.1.2** | **Yes No N/A** | **Remarks:** |
| **29-1.1.3** | **Yes No N/A** | **Remarks:** |
| **29-2** | **Yes No N/A** | **Remarks:** |
| **29-3** | **Yes No N/A** | **Remarks:** |
| **29-4** | **Yes No N/A** | **Remarks:** |
| **29-4.1** | **Yes No N/A** | **Remarks:** |
| **29-4.2** | **Yes No N/A** | **Remarks:** |
| **29-4.3** | **Yes No N/A** | **Remarks:** |
| **29-4.4** | **Yes No N/A** | **Remarks:** |
| **29-4.4.1** | **Yes No N/A** | **Remarks:** |
| **29-4.4.2** | **Yes No N/A** | **Remarks:** |
| **29-4.4.3** | **Yes No N/A** | **Remarks:** |
| **29-4.4.4** | **Yes No N/A** | **Remarks:** |
| **29-5** | **Yes No N/A** | **Remarks:** |
| ***Requirement 30: Physical and logical protections must exist for deployed POI devices.*** | | |
| **30-1** | **Yes No N/A** | **Remarks:** |
| **30-2** | **Yes No N/A** | **Remarks:** |
| ***Requirement 31: Procedures must be in place and implemented to protect any SCDs—and ensure the destruction of any cryptographic keys or key material within such devices—when removed from service, retired at the end of the deployment lifecycle, or returned for repair.*** | | |
| **31-1** | **Yes No N/A** | **Remarks:** |
| **31-1.1** | **Yes No N/A** | **Remarks:** |
| **31-1.2** | **Yes No N/A** | **Remarks:** |
| **31-1.3** | **Yes No N/A** | **Remarks:** |
| **31-1.4** | **Yes No N/A** | **Remarks:** |
| **31-1.5** | **Yes No N/A** | **Remarks:** |
| **31-1.6** | **Yes No N/A** | **Remarks:** |

|  |  |  |
| --- | --- | --- |
| ***Requirement 32: Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:***   * + 1. ***Dual access controls required to enable the key-encryption function***     2. ***Physical protection of the equipment (e.g., locked access to it) under dual control***     3. ***Restriction of logical access to the equipment*** | | |
| **32-1** | **Yes No N/A** | **Remarks:** |
| **32-1.1** | **Yes No N/A** | **Remarks:** |
| **32-1.2** | **Yes No N/A** | **Remarks:** |
| **32-1.3** | **Yes No N/A** | **Remarks:** |
| **32-1.4** | **Yes No N/A** | **Remarks:** |
| **32-1.5** | **Yes No N/A** | **Remarks:** |
| ***Requirement 33: Documented procedures must exist and be demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., POI devices supporting PIN and HSMs) placed into service, initialized, deployed, used, and decommissioned.*** | | |
| **33-1** | **Yes No N/A** | **Remarks:** |

# Normative Annex A – Symmetric Key Distribution using Asymmetric Techniques

# A1 – Remote Key Distribution Using Asymmetric Techniques Operations

## CONTROL OBJECTIVE 1

***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.***

|  |
| --- |
| **No additional security requirements added for “Symmetric Key Distribution using Asymmetric Techniques.”** |

## CONTROL OBJECTIVE 2

***Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.***

|  |
| --- |
| **No additional security requirements added for “Symmetric Key Distribution using Asymmetric Techniques.”** |

## CONTROL OBJECTIVE 3

***Keys are conveyed or transmitted in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 10: All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.*** | | |
| **10-2** | **Yes No N/A** | **Remarks:** |
| **10-3** | **Yes No N/A** | **Remarks:** |
|  |  |  |

## CONTROL OBJECTIVE 4

***Key-loading to hosts and PIN entry devices is handled in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 15: The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*** | | |
| **15-3** | **Yes No N/A** | **Remarks:** |
| **15-5** | **Yes No N/A** | **Remarks:** |
| **15-6** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 5

***Keys are used in a manner that prevents or detects their unauthorized usage.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 18: Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.*** | | |
| **18-4** | **Yes No N/A** | **Remarks:** |
| **18-5** | **Yes No N/A** | **Remarks:** |
| ***Requirement 19: Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*** | | |
| **19-6** | **Yes No N/A** | **Remarks:** |
| **19-7** | **Yes No N/A** | **Remarks:** |
| **19-8** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 6

***Keys are administered in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 21: Secret keys used for enciphering PIN-encryption keys or for PIN encryption, or private keys used in connection with remote key- distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*** | | |
| **21-4** | **Yes No N/A** | **Remarks:** |

# Normative Annex A – Symmetric Key Distribution using Asymmetric Techniques

# A2 – Certification and Registration Authority Operations

## CONTROL OBJECTIVE 3

***Keys are conveyed or transmitted in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 10: All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.*** | | |
| **10-2** | **Yes No N/A** | **Remarks:** |
| **10-3** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 4

***Key-loading to hosts and PIN entry devices is handled in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 15: The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*** | | |
| **15-6** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 5

***Keys are used in a manner that prevents or detects their unauthorized usage.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 19: Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*** | | |
| **19-5** | **Yes No N/A** | **Remarks:** |
| **19-6** | **Yes No N/A** | **Remarks:** |
| **19-9** | **Yes No N/A** | **Remarks:** |
| **19-9.1** | **Yes No N/A** | **Remarks:** |
| **19-10** | **Yes No N/A** | **Remarks:** |
| **19-11** | **Yes No N/A** | **Remarks:** |
| ***Requirement 21: Secret keys used for enciphering PIN-encryption keys or for PIN encryption, or private keys used in connection with remote key- distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*** | | |
| **21-4** | **Yes No N/A** | **Remarks:** |

|  |  |  |
| --- | --- | --- |
| ***Requirement 22: Procedures must exist and be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key.*** | | |
| **22-6** | **Yes No N/A** | **Remarks:** |
| **22-7** | **Yes No N/A** | **Remarks:** |
| **22-7.1** | **Yes No N/A** | **Remarks:** |
| **22-7.2** | **Yes No N/A** | **Remarks:** |
| **22-7.3** | **Yes No N/A** | **Remarks:** |
| **22-7.4** | **Yes No N/A** | **Remarks:** |
| **22-8** | **Yes No N/A** | **Remarks:** |
| ***Requirement 25: Access to secret or private cryptographic keys and key material must be:***   * + 1. ***Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use, and***     2. ***Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.*** | | |
| **25-2** | **Yes No N/A** | **Remarks:** |
| **25-2.1** | **Yes No N/A** | **Remarks:** |
| **25-3** | **Yes No N/A** | **Remarks:** |
| **25-3.1** | **Yes No N/A** | **Remarks:** |
| **25-3.2** | **Yes No N/A** | **Remarks:** |
| **25-3.3** | **Yes No N/A** | **Remarks:** |
| **25-3.4** | **Yes No N/A** | **Remarks:** |
| **25-3.5** | **Yes No N/A** | **Remarks:** |
| **25-4** | **Yes No N/A** | **Remarks:** |
| **25-5** | **Yes No N/A** | **Remarks:** |
| **25-5.1** | **Yes No N/A** | **Remarks:** |
| **25-5.2** | **Yes No N/A** | **Remarks:** |
| **25-6** | **Yes No N/A** | **Remarks:** |
| **25-6.1** | **Yes No N/A** | **Remarks:** |
| **25-6.2** | **Yes No N/A** | **Remarks:** |
| **25-6.3** | **Yes No N/A** | **Remarks:** |
| **25-7** | **Yes No N/A** | **Remarks:** |
| **25-7.1** | **Yes No N/A** | **Remarks:** |
| **25-7.2** | **Yes No N/A** | **Remarks:** |
| **25-8** | **Yes No N/A** | **Remarks:** |
| **25-8.1** | **Yes No N/A** | **Remarks:** |
| **25-8.2** | **Yes No N/A** | **Remarks:** |
| **25-8.3** | **Yes No N/A** | **Remarks:** |
| **25-8.4** | **Yes No N/A** | **Remarks:** |
| **25-8.5** | **Yes No N/A** | **Remarks:** |
| **25-8.6** | **Yes No N/A** | **Remarks:** |
| **25-8.7** | **Yes No N/A** | **Remarks:** |
| **25-8.8** | **Yes No N/A** | **Remarks:** |
| **25-8.9** | **Yes No N/A** | **Remarks:** |
| **25-9** | **Yes No N/A** | **Remarks:** |
| ***Requirement 28: Documented procedures must exist and be demonstrably in use for all key-administration operations.*** | | |
| **28-2** | **Yes No N/A** | **Remarks:** |
| **28-3** | **Yes No N/A** | **Remarks:** |
| **28-4** | **Yes No N/A** | **Remarks:** |
| **28-5** | **Yes No N/A** | **Remarks:** |
| **28-5.1** | **Yes No N/A** | **Remarks:** |
| **28-5.2** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 7

***Equipment used to process PINs and keys is managed in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 32: Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:***   * + 1. ***Dual access controls are required to enable the key-encryption function.***     2. ***Physical protection of the equipment (e.g., locked access to it) under dual control.***     3. ***Restriction of logical access to the equipment*** | | |
| **32-2.1** | **Yes No N/A** | **Remarks:** |
| **32-2.2** | **Yes No N/A** | **Remarks:** |
| **32-2.2.1** | **Yes No N/A** | **Remarks:** |
| **32-2.2.2** | **Yes No N/A** | **Remarks:** |
| **32-2.2.3** | **Yes No N/A** | **Remarks:** |
| **32-2.3** | **Yes No N/A** | **Remarks:** |
| **32-2.3.1** | **Yes No N/A** | **Remarks:** |
| **32-2.3.2** | **Yes No N/A** | **Remarks:** |
| **32-2.4** | **Yes No N/A** | **Remarks:** |
| **32-2.5** | **Yes No N/A** | **Remarks:** |
| **32-2.5.1** | **Yes No N/A** | **Remarks:** |
| **32-2.5.2** | **Yes No N/A** | **Remarks:** |
| **32-2.6** | **Yes No N/A** | **Remarks:** |
| **32-2.6.1** | **Yes No N/A** | **Remarks:** |
| **32-2.6.2** | **Yes No N/A** | **Remarks:** |
| **32-2.7** | **Yes No N/A** | **Remarks:** |
| **32-2.7.1** | **Yes No N/A** | **Remarks:** |
| **32-2.7.2** | **Yes No N/A** | **Remarks:** |
| **32-2.7.3** | **Yes No N/A** | **Remarks:** |
| **32-2.7.4** | **Yes No N/A** | **Remarks:** |
| **32-2.8** | **Yes No N/A** | **Remarks:** |
| **32-2.8.1** | **Yes No N/A** | **Remarks:** |
| **32-2.9** | **Yes No N/A** | **Remarks:** |
| **32-2.9.1** | **Yes No N/A** | **Remarks:** |
| **32-2.9.2** | **Yes No N/A** | **Remarks:** |
| **32-2.9.3** | **Yes No N/A** | **Remarks:** |
| **32-2.9.4** | **Yes No N/A** | **Remarks:** |
| **32-2.9.5** | **Yes No N/A** | **Remarks:** |
| **32-2.9.6** | **Yes No N/A** | **Remarks:** |
| **32-2.9.7** | **Yes No N/A** | **Remarks:** |
| **32-3** | **Yes No N/A** | **Remarks:** |
| **32-3.1** | **Yes No N/A** | **Remarks:** |
| **32-3.2** | **Yes No N/A** | **Remarks:** |
| **32-3.3** | **Yes No N/A** | **Remarks:** |
| **32-3.4** | **Yes No N/A** | **Remarks:** |
| **32-4** | **Yes No N/A** | **Remarks:** |
| **32-4.1** | **Yes No N/A** | **Remarks:** |
| **32-4.2** | **Yes No N/A** | **Remarks:** |
| **32-5** | **Yes No N/A** | **Remarks:** |
| **32-6** | **Yes No N/A** | **Remarks:** |
| **32-6.1** | **Yes No N/A** | **Remarks:** |
| **32-6.2** | **Yes No N/A** | **Remarks:** |
| **32-6.3** | **Yes No N/A** | **Remarks:** |
| **32-7** | **Yes No N/A** | **Remarks:** |
| **32-7.1** | **Yes No N/A** | **Remarks:** |

# Normative Annex B – Key-Injection Facilities

# Key-Injection Facility Security Requirements Technical Reference

## CONTROL OBJECTIVE 1

***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 1: All cardholder-entered PINs must be processed in equipment that conforms to the requirements for secure cryptographic devices (SCDs). PINs must never appear in the clear outside of an SCD.*** | | |
| **1-2** | **Yes No N/A** | **Remarks:** |
| **1-3** | **Yes No N/A** | **Remarks:** |
| **1-4** | **Yes No N/A** | **Remarks:** |
| **1-5** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 2

***Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 5: All keys and key components must be generated using an approved random or pseudo-random process.*** | | |
| **5-1** | **Yes No N/A** | **Remarks:** |
| ***Requirement 6: Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.*** | | |
| **6-1** | **Yes No N/A** | **Remarks:** |
| **6-1.1** | **Yes No N/A** | **Remarks:** |
| **6-1.2** | **Yes No N/A** | **Remarks:** |
| **6-1.3** | **Yes No N/A** | **Remarks:** |
| **6-1.4** | **Yes No N/A** | **Remarks:** |
| **6-1.5** | **Yes No N/A** | **Remarks:** |
| **6-2** | **Yes No N/A** | **Remarks:** |
| **6-3** | **Yes No N/A** | **Remarks:** |
| **6-4** | **Yes No N/A** | **Remarks:** |
| **6-5** | **Yes No N/A** | **Remarks:** |
| **6-6** | **Yes No N/A** | **Remarks:** |
| ***Requirement 7: Documented procedures must exist and be demonstrably in use for all key-generation processing.*** | | |
| **7-1** | **Yes No N/A** | **Remarks:** |
| **7-2** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 3

***Keys are conveyed or transmitted in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 8: Secret or private keys must be transferred by:***   * 1. ***Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or***   2. ***Transmitting the key in ciphertext form.***   ***Public keys must be conveyed in a manner that protects their integrity and authenticity.*** | | |
| **8-1** | **Yes No N/A** | **Remarks:** |
| **8-2** | **Yes No N/A** | **Remarks:** |
| **8-3** | **Yes No N/A** | **Remarks:** |
| **8-4** | **Yes No N/A** | **Remarks:** |
| ***Requirement 9: During its transmission, conveyance, or movement between any two organizational entities, any single unencrypted secret or private key component must at all times be protected.***  ***Sending and receiving entities are equally responsible for the physical protection of the materials involved.*** | | |
| **9-1** | **Yes No N/A** | **Remarks:** |
| **9-2** | **Yes No N/A** | **Remarks:** |
| **9-3** | **Yes No N/A** | **Remarks:** |
| **9-4** | **Yes No N/A** | **Remarks:** |
| **9-5** | **Yes No N/A** | **Remarks:** |
| ***Requirement 10:******All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.*** | | |
| **10-1** | **Yes No N/A** | **Remarks:** |
| ***Requirement 11: Documented procedures must exist and be demonstrably in use for all key transmission and conveyance processing.*** | | |
| **11-1** | **Yes No N/A** | **Remarks:** |
| **11-2** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 4

***Key-loading to hosts and PIN entry devices is handled in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 12: Secret and private keys must be input into hardware (host) security modules (HSMs) and PIN entry devices (PEDs) in a secure manner.***   * + 1. ***Unencrypted secret or private keys must be entered using the principles of dual control and split knowledge.***     2. ***Key-establishment techniques using public-key cryptography must be implemented securely.*** | | |
| **12-1** | **Yes No N/A** | **Remarks:** |
| **12-2** | **Yes No N/A** | **Remarks:** |
| **12-3** | **Yes No N/A** | **Remarks:** |
| **12-4** | **Yes No N/A** | **Remarks:** |
| **12-5** | **Yes No N/A** | **Remarks:** |
| **12-6** | **Yes No N/A** | **Remarks:** |
| **12-7** | **Yes No N/A** | **Remarks:** |
| **12-8** | **Yes No N/A** | **Remarks:** |
| **12-9** | **Yes No N/A** | **Remarks:** |
| ***Requirement 13: The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.*** | | |
| **13-1** | **Yes No N/A** | **Remarks:** |
| **13-2** | **Yes No N/A** | **Remarks:** |
| **13-3** | **Yes No N/A** | **Remarks:** |
| **13-4** | **Yes No N/A** | **Remarks:** |
| **13-4.1** | **Yes No N/A** | **Remarks:** |
| **13-4.2** | **Yes No N/A** | **Remarks:** |
| **13-4.3** | **Yes No N/A** | **Remarks:** |
| **13-4.4** | **Yes No N/A** | **Remarks:** |
| **13-5** | **Yes No N/A** | **Remarks:** |
| **13-6** | **Yes No N/A** | **Remarks:** |
| **13-7** | **Yes No N/A** | **Remarks:** |
| **13-8** | **Yes No N/A** | **Remarks:** |
| **13-9** | **Yes No N/A** | **Remarks:** |
| **13-9.1** | **Yes No N/A** | **Remarks:** |
| **13-9.2** | **Yes No N/A** | **Remarks:** |
| **13-9.3** | **Yes No N/A** | **Remarks:** |
| **13-9.4** | **Yes No N/A** | **Remarks:** |
| **13-9.4.1** | **Yes No N/A** | **Remarks:** |
| **13-9.4.2** | **Yes No N/A** | **Remarks:** |
| **13-9.4.3** | **Yes No N/A** | **Remarks:** |
| **13-9.4.4** | **Yes No N/A** | **Remarks:** |
| **13-9.4.5** | **Yes No N/A** | **Remarks:** |
| **13-9.4.6** | **Yes No N/A** | **Remarks:** |
| **13-9.4.7** | **Yes No N/A** | **Remarks:** |
| **13-9.4.8** | **Yes No N/A** | **Remarks:** |
| **13-9.4.9** | **Yes No N/A** | **Remarks:** |
| **13-9.4.10** | **Yes No N/A** | **Remarks:** |
| ***Requirement 14: All hardware and access/authentication mechanisms (e.g., passwords) used for key loading must be managed under the principle of dual control.*** | | |
| **14-1** | **Yes No N/A** | **Remarks:** |
| **14-2** | **Yes No N/A** | **Remarks:** |
| **14-3** | **Yes No N/A** | **Remarks:** |
| **14-4** | **Yes No N/A** | **Remarks:** |
| **14-5** | **Yes No N/A** | **Remarks:** |
| ***Requirement 15: The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*** | | |
| **15-1** | **Yes No N/A** | **Remarks:** |
| **15-2** | **Yes No N/A** | **Remarks:** |
| ***Requirement 16: Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.*** | | |
| **16-1** | **Yes No N/A** | **Remarks:** |
| **16-2** | **Yes No N/A** | **Remarks:** |
| *Requirement 18: Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.* | | |
| **18-2** | **Yes No N/A** | **Remarks:** |
| **18-3** | **Yes No N/A** | **Remarks:** |
| **18-4** | **Yes No N/A** | **Remarks:** |
| **18-5** | **Yes No N/A** | **Remarks:** |
| ***Requirement 19: Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*** | | |
| **19-1** | **Yes No N/A** | **Remarks:** |
| **19-2** | **Yes No N/A** | **Remarks:** |
| **19-3** | **Yes No N/A** | **Remarks:** |
| **19-4** | **Yes No N/A** | **Remarks:** |
| **19-5** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 5

***Keys are used in a manner that prevents or detects their unauthorized usage.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 20: All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (e.g., PED) that processes PINs must be unique (except by chance) to that device.*** | | |
| **20-1** | **Yes No N/A** | **Remarks:** |
| **20-2** | **Yes No N/A** | **Remarks:** |
| **20-3** | **Yes No N/A** | **Remarks:** |
| **20-4** | **Yes No N/A** | **Remarks:** |
| **20-5** | **Yes No N/A** | **Remarks:** |
| **20-6** | **Yes No N/A** | **Remarks:** |
| ***Requirement 21: Secret keys used for enciphering PIN-encryption keys or for PIN encryption, or private keys used in connection with remote key- distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*** | | |
| **21-1** | **Yes No N/A** | **Remarks:** |
| **21-2** | **Yes No N/A** | **Remarks:** |
| **21-2.1** | **Yes No N/A** | **Remarks:** |
| **21-2.2** | **Yes No N/A** | **Remarks:** |
| **21-2.3** | **Yes No N/A** | **Remarks:** |
| **21-2.4** | **Yes No N/A** | **Remarks:** |
| **21-3** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 6

***Keys are administered in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 21: Secret keys used for enciphering PIN-encryption keys or for PIN encryption, or private keys used in connection with remote key- distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*** | | |
| **21-1** | **Yes No N/A** | **Remarks:** |
| **21-2** | **Yes No N/A** | **Remarks:** |
| **21-2.1** | **Yes No N/A** | **Remarks:** |
| **21-2.2** | **Yes No N/A** | **Remarks:** |
| **21-2.3** | **Yes No N/A** | **Remarks:** |
| **21-2.4** | **Yes No N/A** | **Remarks:** |
| **21-3** | **Yes No N/A** | **Remarks:** |
| **21-3.1** | **Yes No N/A** | **Remarks:** |
| **21-3.2** | **Yes No N/A** | **Remarks:** |
| **21-3.3** | **Yes No N/A** | **Remarks:** |
| ***Requirement 22: Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key, its subsidiary keys (those keys encrypted with the compromised key), and keys derived from the compromised key, to a value not feasibly related to the original key.*** | | |
| **22-1** | **Yes No N/A** | **Remarks:** |
| **22-1.1** | **Yes No N/A** | **Remarks:** |
| **22-1.2** | **Yes No N/A** | **Remarks:** |
| **22-1.3** | **Yes No N/A** | **Remarks:** |
| **22-1.4** | **Yes No N/A** | **Remarks:** |
| **22-1.5** | **Yes No N/A** | **Remarks:** |
| **22-2** | **Yes No N/A** | **Remarks:** |
| ***Requirement 23: Keys generated using reversible key-calculation methods, such as key variants, must only be used in SCDs that possess the original key.*** | | |
| **23-1** | **Yes No N/A** | **Remarks:** |
| **23-2** | **Yes No N/A** | **Remarks:** |
| **23-3** | **Yes No N/A** | **Remarks:** |
| ***Requirement 24: Secret and private keys and key components that are no longer used or have been replaced must be securely destroyed.*** | | |
| **24-1** | **Yes No N/A** | **Remarks:** |
| **24-2** | **Yes No N/A** | **Remarks:** |
| **24-2.1** | **Yes No N/A** | **Remarks:** |
| **24-2.2** | **Yes No N/A** | **Remarks:** |
| **24-2.3** | **Yes No N/A** | **Remarks:** |
| ***Requirement 25: Access to secret and private cryptographic keys and key material must be:***   * + 1. ***Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and***     2. ***Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.*** | | |
| **25-1** | **Yes No N/A** | **Remarks:** |
| **25-1.1** | **Yes No N/A** | **Remarks:** |
| **25-1.2** | **Yes No N/A** | **Remarks:** |
| **25-1.3** | **Yes No N/A** | **Remarks:** |
| **25-1.4** | **Yes No N/A** | **Remarks:** |
| ***Requirement 26: Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD.*** | | |
| **26-1** | **Yes No N/A** | **Remarks:** |
| ***Requirement 27: Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.***  ***Note: It is not a requirement to have backup copies of key components or keys.*** | | |
| **27-1** | **Yes No N/A** | **Remarks:** |
| **27-2** | **Yes No N/A** | **Remarks:** |
| ***Requirement 28: Documented procedures must exist and be demonstrably in use for all key-administration operations.*** | | |
| **28-1** | **Yes No N/A** | **Remarks:** |
| ***Requirement 29: PIN-processing equipment (e.g., POI devices and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the deployment of the device—both prior to and subsequent to the loading of cryptographic keys—and that precautions are taken to minimize the threat of compromise once deployed.*** | | |
| **29-1** | **Yes No N/A** | **Remarks:** |
| **29-1.1** | **Yes No N/A** | **Remarks:** |
| **29-1.2** | **Yes No N/A** | **Remarks:** |
| **29-1.3** | **Yes No N/A** | **Remarks:** |
| **29-2** | **Yes No N/A** | **Remarks:** |
| **29-3** | **Yes No N/A** | **Remarks:** |
| **29-4** | **Yes No N/A** | **Remarks:** |
| **29-4.1** | **Yes No N/A** | **Remarks:** |
| **29-4.2** | **Yes No N/A** | **Remarks:** |
| **29-4.3** | **Yes No N/A** | **Remarks:** |
| **29-4.4** | **Yes No N/A** | **Remarks:** |
| **29-4.4.1** | **Yes No N/A** | **Remarks:** |
| **29-4.4.2** | **Yes No N/A** | **Remarks:** |
| **29-4.4.3** | **Yes No N/A** | **Remarks:** |
| **29-4.4.4** | **Yes No N/A** | **Remarks:** |
| **29-5** | **Yes No N/A** | **Remarks:** |

## CONTROL OBJECTIVE 7

***Equipment used to process PINs and keys is managed in a secure manner.***

|  |  |  |
| --- | --- | --- |
| ***Requirement 30: Physical and logical protections must exist for deployed POI devices.*** | | |
| **30-3** | **Yes No N/A** | **Remarks:** |
| ***Requirement 31: Procedures must be in place and implemented to protect any SCDs—and ensure the destruction of any cryptographic keys or key material within such devices—when removed from service, retired at the end of the deployment lifecycle, or returned for repair.*** | | |
| **31-1** | **Yes No N/A** | **Remarks:** |
| **31-1.1** | **Yes No N/A** | **Remarks:** |
| **31-1.2** | **Yes No N/A** | **Remarks:** |
| **31-1.3** | **Yes No N/A** | **Remarks:** |
| **31-1.4** | **Yes No N/A** | **Remarks:** |
| **31-1.5** | **Yes No N/A** | **Remarks:** |
| **31-1.6** | **Yes No N/A** | **Remarks:** |
| ***Requirement 32: Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:***   * + - 1. ***Dual access controls required to enable the key-encryption function***       2. ***Physical protection of the equipment (e.g., locked access to it) under dual control***       3. ***Restriction of logical access to the equipment*** | | |
| **32-1** | **Yes No N/A** | **Remarks:** |
| **32-1.1** | **Yes No N/A** | **Remarks:** |
| **32-1.2** | **Yes No N/A** | **Remarks:** |
| **32-1.3** | **Yes No N/A** | **Remarks:** |
| **32-1.4** | **Yes No N/A** | **Remarks:** |
| **32-1.5** | **Yes No N/A** | **Remarks:** |
| **32-9** | **Yes No N/A** | **Remarks:** |
| **32-9.1** | **Yes No N/A** | **Remarks:** |
| **32-9.2** | **Yes No N/A** | **Remarks:** |
| **32-9.3** | **Yes No N/A** | **Remarks:** |
| **32-9.4** | **Yes No N/A** | **Remarks:** |
| **32-9.5** | **Yes No N/A** | **Remarks:** |
| **32-9.6** | **Yes No N/A** | **Remarks:** |
| **32-9.7** | **Yes No N/A** | **Remarks:** |
| **32-10** | **Yes No N/A** | **Remarks:** |
| **32-10.1** | **Yes No N/A** | **Remarks:** |
| **32-10.2** | **Yes No N/A** | **Remarks:** |
| **32-10.3** | **Yes No N/A** | **Remarks:** |
| **32-10.4** | **Yes No N/A** | **Remarks:** |
| **32-10.5** | **Yes No N/A** | **Remarks:** |
| **32-10.6** | **Yes No N/A** | **Remarks:** |
| **32-10.7** | **Yes No N/A** | **Remarks:** |
| **32-10.8** | **Yes No N/A** | **Remarks:** |
| **32-10.9** | **Yes No N/A** | **Remarks:** |
| **32-10.10** | **Yes No N/A** | **Remarks:** |
| **32-10.11** | **Yes No N/A** | **Remarks:** |
| ***Requirement 33: Documented procedures must exist and be demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., POI devices supporting PIN and HSMs) placed into service, initialized, deployed, used, and decommissioned.*** | | |
| **33-1** | **Yes No N/A** | **Remarks:** |

# PCI PIN Security Requirements Exception Form

An individual Exception Form must be submitted for each statement on the PCI PIN Security Requirements item for which you did not respond “Yes”. The Chief/General Internal Auditor or an independent outside auditor must attest to this form.

|  |  |  |  |
| --- | --- | --- | --- |
| **Organization Information** | | | |
| Company Name: |  | Title: |  |
| Contact Name: |  | E-mail: |  |
| Telephone: |  | Fax: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Date: |  | Submitted for Year of: | Or Start-up Date: |

|  |
| --- |
| PCI Security Requirement: |

|  |
| --- |
| Explain why the PCI Security Requirement could not be answered “Yes”: |

|  |
| --- |
| Describe the action plan that will be implemented to correct this situation: |

|  |
| --- |
| Date expected to be in compliance: |

|  |
| --- |
| Auditor signature: |